ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

Vol. 3, Issue 2, February 2015

# Attack Graph Model: A New Approach for DDOS Attack Detection in Cloud

R.Jeena[1] M.Rajeswari[2]

Assistant Professor, Dept. of I.T., Panimalar Institute of Technology, Chennai, India[1&2]

**ABSTRACT**: Cloud computing is an up-and-coming area that affects IT infrastructure, network services, and applications. In cloud computing the current adoption is associated with numerous challenges like security, performance, availability, etc. In this distributed model, the infrastructure is shared by potentially millions of users. Distributed Denial of Service (DDOS) attack has the potential to have greater impact in cloud computing. In this paper to prevent the vulnerable virtual machine from being compromised in the cloud, we purpose an attack graph model. This model is the easiest way to show all possible attack paths of the host in cloud that is crucial to understand threats.

**KEYWORDS**: Cloud computing; attack graph; intrusion detection

## I. INTRODUCTION

Cloud computing is an up-and-coming IT delivery model, used to describe a new class of networking computing. It which can deliver both software and hardware as on-demand resources and services over the internet with lower IT complexities and cost[1].

**Software as a service (saas).** The Capability provided to users on cloud to use an application of provider that are running on a cloud infrastructure and accessible from various client devices through a thin-client interface such as a web browser. It offers application like Google doc to end users to use on the cloud vendors.

**Platform as a Service (PaaS).**The Capability provided to the consumer is to deploy onto the cloud infrastructure.Consumer creating application using programming language and tools supported by the provider. Cloud vendors offerPaaS services like Google App Engine to allow users to host their applications instead of buying new resources to house them.

**Infrastructure as a Service (IaaS).** The capability provided to the cloud user is to provision storage, networks, processing and other fundamental computing resources where the consumer is able to deploy and run arbitrary software.It is sometimes called everything as a service.

Fig.1 Cloud Computing

**Public cloud.** It services through the Internet. It offers IT resources and services to individuals and businesses to save the overhead of having in house built resources

**Community cloud.** The Specific community of organization who have common concerns can share their cloud infrastructure to collaborate forming a community cloud.

**Private cloud.**The services are restricted to only those who own the clouds and their subsidiaries.

**Hybrid cloud.** Connecting public and private cloud but are bound together by standardized or proprietary technology.

## II. RELATED WORK

In this section, we present literatures of several highly related areas to this project including: intrusion detection and prevention, attack graph construction and security analysis.

The impact score of vulnerability is defined in the CVSS guide [7] helps to judge the confidentiality, integrity and availability impact of the vulnerabilities being exploited.

In [8] researchers are interested in distributing the IDS among the nodes of the grid within cloud computing environment in order to monitor each node and alert the other nodes when an attack occurs. They proposed Grid and Cloud Computing Intrusion Detection System (GCCIDS) which is designed to cover the attacks that network and host based systems cannot detect. There proposed method used the integration of knowledge and behavior analysis to detect specific instructions. But the proposed prototype cannot discover new types of attacks or create an attack database which must be considered during implementing IDS.

In a general DDoS attack, the attacker usually disguises or ‘spoofs’ the IP address section of a packet header in order to hide their identity from their victim. This makes it extremely difficult to trace the source of the attack. IP trace back is the scheme that provides an effective way to trace the source of DDoS attacks to its point of origin [9].

The scenario attack graph is proposed to find all relationship between the attack paths. Vulnerability in attack graph means that the alert is more likely to be a real attack. This will not increase the false positive rate. The vulnerability is detected by the attacker but is not detected by vulnerability scanner. In such case the alert being real will be regarded as false, so false negative rate increase [10].

A new multithreaded distributed cloud IDS was proposes to handle largely connected network access traffic and administrative control of data and application in cloud. This handles large flow of data packets, analyze them and generate reports efficiently by integrating knowledge and behavior analysis to detect intrusions. [10]

## III. IDS IN CLOUD

### A.Intrusion Detection System

Intrusion detection systems are software or hardware systems that automaticallymonitoring the computer system or network events and analyze them for malicious activities or policy violations and produces reports to a management station.

**Types**

1. **Host based IDS (HIDS)** which monitors specific machines.
2. **Network based IDS (NIDS)** which identifies intrusions on key network points.
3. **Distributed IDS (DIDS)** which operates both host as well as network

**Functionalities**

1. Monitoring and analyzing both user and system activities.
2. Analyzing system configurations and vulnerabilities.
3. Accessing system file and integrity.
4. Ability to recognize patterns typical of attacks
5. Analysis of abnormal activity patterns
6. Tracking user policy violations.

### B. Cloud IDS

IDS in cloud environment [2] can be both network and host based. Network based IDS analyses. The IDS placed in network switch and capture packet in real time.

## IV. PROPOSED ALGORITHM

This paper focus on provides security to virtual machines in the cloud system. Enhanced intrusion detection is proposed to provide security to cloud nodes by detecting DDOS attack. The IDS is placed in the network switch to monitor all activities of nodes in cloud system. An attack graph is generated to find all possible attack paths. In the proposed system the details about users of the cloud system is stored in the service registry. Whenever the user access service, the details are registered. If the sending data rate is greater than the threshold the alert is generated and the attack graph model is constructed. The system captures and inspects suspicious cloud traffic. It can improve the attack detection probability and improve the resiliency to VM exploitation attack without interrupting existing normal cloud services. False negative rate is avoided by perfectly scanning the vulnerability.

There are many ways to find solution for a particular problem. It is always necessary to find the best optimal solution. The best optimal solution depends on the type of problem. As of the project it is necessary to increase the security in cloud computing. For this purpose three major Security Detection processes are carried out.

The first process is the VMprofiling; this process is used to scan all virtual machines in the cloud. The running virtual machinesare listed from the cloud. After that the details of all virtual machines are collected. The details include the VM name, IP address, CPU, memory space, OS. From this process we can easily view all VM details.

The second process is detecting the infected nodes. For finding the infected node several processes take place. The processes are packet monitoring, user behavior monitoring etc. Packet monitoring for finding the infected node is done by checking the incoming packets, whether it contains any malicious code or data. Data rate checking means which user sends more data rate than the threshold value. Because the normal user only send data’s to the needed nodes but the attacker try to affect all nodes in the network connections so automatically the data rate increase. The next process is the attacker sends more packets to the target node. So the target node traffic is always busy. So the other node can’t get service from the target node. Such we find the vulnerability and infected node details from this process.

The third process is the attack graph generation. After finding the infected node then the attack graph is generated.. Each path from an initial node to target node represent successful attack. Attack graph is helpful in identifying potential threats, possible attacks, and known vulnerabilities in a cloud. Implementing this concept has good possibilities of reducing false alarms. This project can be implemented using VMware.

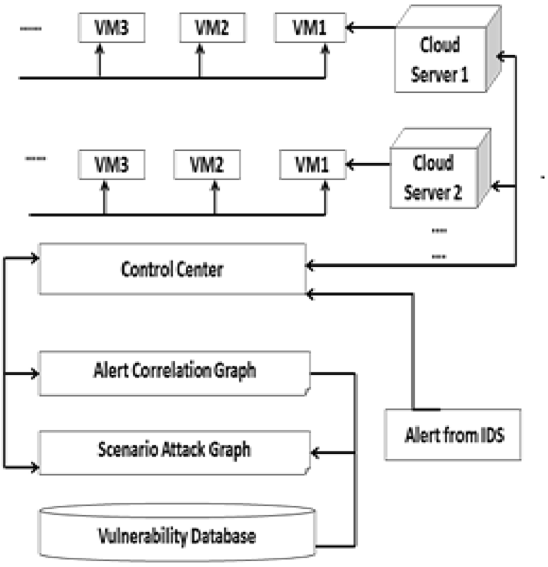

Fig.2Architecture Diagram

The architecture diagram defines the working process of the proposed system.

## V. SIMULATION RESULTS

### Attack Graph Model

Attack Graph Model is used to illustrate all possible multihost attack paths. The attack paths are used to understand threads and then decide appropriate counter measures. A graph is constructed in which nodes represent state of attack and edges represent the correlations between attacks. Each node in the attack graph represents either precondition or consequence of an exploit. It is helping to identify potential threats, possible attacks and known vulnerabilities in a cloud system.

### 1. Scenario Attack Graph(SAG)

An SAG is a tuple SAG= (V, E), where

**a.** V=$N_C \cup N_D \cup N_R$ these are set of vertices named conjunction node, disjunction node and root node.

**b.** E=$E_{pre}$U$E_{post}$ these are directed edges. An edge e$\in E_{pre} \subseteq N_D \times N_C$ means $N_D$ must be satisfied to achieve$N_C$. An edge e$\in E_{post} \subseteq N_C \times N_D$ represents $N_D$ can be obtained if $N_C$ is satisfied.

### 2. Attack Correlation Graph(ACG)

An ACG has three tuple ACG= (A, E, P) where

a. A is a set of aggregated alerts. An alert a$\in$A is a data structure represents source IP address, destination IP address, type of alert and time stamp of alert.

b. Alerts map to a pair of vertices ($v_c, v_d$) in SAG using map (a) function.
Map(a):a→{($v_c \times v_d$) | (a.src$\in v_c$.Hosts)$\wedge$(a.dst$\in v_d$.Hosts)$\wedge$(a.cls=$v_c$.vul)}.

c. E is a set of directed edges representing correlation between two alerts(a,$a'$) if criteria below is satisfied:

i. .(a..ts)$\wedge$($a'$.ts)$\wedge$ $a'$.ts-a.ts<threshold).

ii. $\exists$(($v_d, v_c$)$\in E_{pre}$: (a.dst$\in v_d$.Hosts$\wedge$ $a'$.src$\in v_c$.Hosts).

d. P is set of paths in ACG. A path $S_i \subset$P is a set of related alerts in chronological order.

e.

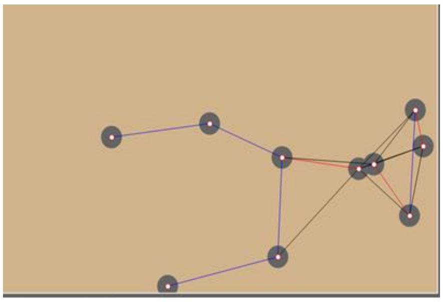

Fig.3. Attack Graph Diagram

### A. Counter Measure Selection

When the vulnerabilities are discovered or some VMs are identified as suspicious, several countermeasures can be taken to restrict attacker's capabilities and it is important to differentiate between compromised and suspicious VMs.The countermeasure serves the purpose of 1) protecting the target VMs from being compromised and making attack behavior stand prominent so that the attacker’s actions can be modified.

TABLE
SOME POSSIBLE COUNTER MEASURE TYPES

| No | Countermeasures |
|---|---|
| 1 | Block Port |
| 2 | Creating Filter rules |
| 3 | Deep Packet Inspection |
| 4 | IP address change |
| 5 | MAC address change |
| 6 | Networktopology change |
| 7 | Network reconfiguration |
| 8 | Software patch |
| 9 | Traffic isolation |
| 10 | Traffic redirection |
| 11 | Quarantine |

## VI. CONCLUSION AND FUTURE WORK

This work is proposed to detect and mitigate the collaborative attacks in the cloud virtual networking environment. It utilizes the attack graph model to conduct attack detection and prediction. It improves the detection accuracy, and defect victim exploitation phases of collaborative attacks. This solution can significantly reduce the risk of the cloud system from being exploited and abused by internal and external attackers.

## REFERENCES

1. M.Armbrust,A.Fox,R.Griffith,AnthonyD.Joseph,et al. “About the Clouds: A Berkeley View of Cloud Computing”. 2009, EECS Department, University of California, Berkeley.
2. S.N Dhage, B BMeshram, R Rawat, “Intrusion Detection System in cloud environment”, International Conference an Workshop on Emerging Trends in Technology (ICWET 2011) _TCET, Mumbai, India”.
3. Bouzida Y, Cuppens F, Gombault S, (2006),”Detecting and Reacting against Distributed Denial of Service Attacks,” IEEE International Conference on Communication Volume 5
4. IfikharA,Azween B.A., Abdullah S.A(2009).,”Application of Artificial neural Network in Detection of Dos attacks,”Sin’09,Oct 6-10
5. Trostle J,(2006),”Protecting Against Distributed Denial of service attacks Using Distributed Filtering,” Securecomm and Workshops, Aug 28 2006-septl 2006,pp 1-11.
6. H.Takabi, J.B.Joshi, and G.Ahn, “Security and Privacy Challenges in Cloud Computing Environments,” IEEE Security and Privacy, vol.8, no.6, pp. 24-31, Dec.2010.
7. P.Mell,K.Scarfone and S.Romanosky, “Common Vulnerability Scoring System(CVSS),” http://www.first.org/cvss/cvss-guide.html,May 2010.
8. K.Vieira, A.Schulter, C.B.Westphall and C.M.Westpall, “Intrusion Detection for Grid and Cloud Computing”, IT Professional, Volume:12 Issuse:4, pp.38-43, 2010
9. B.Joshi, A.Vijayan, and B.Joshi, “Securing Cloud Computing Environment Against s DDoS Attacks,”Proc. IEEE Int’l Conf. Computer Comm. and Informatics(ICCCI’12), Jan.2012
10. Chun-Jen Chung, PankajKhatkar, Tianyi Xing Jeongkeun Lee, Dijiang Huang, “NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems”, IEEE Transactions On Dependable And Secure Computing, Vol. 10, No. 4, July/August 2013
11. Ms.ParagK.Shelke, Ms.SnehaSontakke, Dr.A.D.Gawande, “Intrusion Detection System for Cloud Computing”, International journal of Scientific & Technology Research Volume 1, Issue 4, May 2012.

## BIOGRAPHY

**Jeena R** is an Assistant Professor in the Department of Information Technology, Panimalar Institute of Technology, Chennai. She received Master of Engineering (ME) degree in 2011 from Vel Tech University, Chennai. Her research interests are Cloud computing, wireless Networks, Big Data, etc.

**Rajeswari M** is an Assistant Professor in the Department of Information Technology, Panimalar Institute of Technology, Chennai. She received Master of Engineering (ME) degree in 2013 from St.Perter’s University, Chennai. Her research interests are Cloud Computing, Data Mining, Computer Networks, etc.